

**Privacy & Security Workgroup**  
**Draft Transcript**  
**June 17, 2010**

**Presentation**

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Great, thank you. Good morning, everybody, and welcome to the Privacy and Security Workgroup Webinar this morning. Let me do a quick roll call. Dixie Baker?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

I'm here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Anne Castro? Steve Findlay? David McCallie?

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Present.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Wes Rishel?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Jim Bialick?

**Jim Bialick – Genetic Alliance – Health Systems Coordinator**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Walter Suarez? Aneesh Chopra? John Moehrke? Ed Larson? Judy Faulkner?

**Judy Faulkner – Epic Systems – Founder**

Here.

**Judy Sparrow – Office of the National Coordinator – Executive Director**

Anybody else from the Privacy and Security Policy Workgroup? Okay, I'll turn it over to Dixie.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay. Today is the last of our educational sessions or at least the last one that has been planned around the topic of management of consumer consents or consumer permissions. At the last session we heard about the HL-7 work around consent directives and the management of consent directives, the creation of consent directives. And today I'm very pleased to have Mike Davis from the VA, the Veterans Health Administration, and David Staggs from SAIC, who is supporting Mike Davis at the VA. They're doing a pilot around the consents that we heard at the HL-7 presentation. So with that, I'll turn it over to you, Mike.

**Mike Davis – Veterans Health Administration – Security Architect**

Thank you very much, Dixie. As Dixie said, I'm very pleased to be able to address this group today and I appreciate you inviting us. I'm the security architect and lead for security standards efforts within the

health administration of the Department of Veterans Affairs, and I'm also co-chair of the HL-7 Security Workgroup. With me is David Staggs, who I'll allow to introduce himself.

**David Staggs – SAIC – Consultant**

Thanks Mike. Yes, my name is David Staggs, I'm a SAIC Consultant engaged with the Department of Veterans Affairs. I am a co-chair of the OASIS cross enterprise security and privacy TC. And I'm currently involved in the VA pilot project demonstrating the use of the NHIN for the exchange of clinical data.

**Mike Davis – Veterans Health Administration – Security Architect**

This presentation is around the topic of implementing advance security and privacy in the NHIN from a security practitioner's viewpoint. We think it's advanced because it does employ underlying security and privacy standards that have in some cases only recently have been validated within their respective standards development organization; or because of the use of technology framework, it's not in general use in healthcare. Our frameworks that are now just being demonstrating this capability and have only recently been considered for pilot projects.

We hope here to demonstrate that the core technologies are themselves fundamentally practical and that they can meet current and future security and privacy needs within the healthcare community, and without the need to throw out existing systems. Furthermore, there are a number of existing interoperable solutions from major vendors capable of meeting these advance security and privacy concepts within the context of the NHIN.

There are clearly a number of issues around policy that are significant and we're not going to attempt to address them directly here; although, there may be references to them. To be clear, when I speak of policy in general for the most part, we mean the rules implemented in systems rather than the laws that drive them. So rather than enforcing a static policy, our approach is to implement a system capable of enforcing many policies, and therefore it is adaptive. By way of agenda, we will discuss the introduction, which we just did, foundations for what we're talking about, implementation. We'll walk through a demonstration and then a summary at the end.

On this slide, we're talking about the motivation through VA. This is how VA is doing things, but we're doing them through standards development organizations and through the NHIN. Last year, President Obama announced the virtual lifetime electronic record project capability within DoD and the VA. Behind the President is Secretary Gates and Secretary Eric Shinseki of the VA.

This project is the VA's project to create interoperability between the VA and DoD. Within the VA, the VLER project ranks fourth among 13 top priority projects. And the NHIN standards and functionality is being used to implement VLER. VA currently has NHIN projects currently active with Kaiser in San Diego sharing live data with plans for VA/DoD sharing in Hampton, VA area. VA for a number of years has shared information electronically with the DoD and we share a special relationship with them, both in terms of the population served and is specified in law in USC Title 38.

We have about 6.5 million veterans eligible for care, currently actively receiving care in the VA. Interestingly enough, about 75% to 80% of the VA patients under 65 years of age, and 85% of VA patients over age 65 receive some healthcare services outside of VA. Of these patients in the San Diego area with Kaiser Permanente, they treat about 1,200 veterans in San Diego, shared with the San Diego VA Medical Center.

This slide here refers to a description of the San Diego project. If you click on the link there, the news report link, it'll bring up a news video from Channel 5 Fox News in the San Diego area that aired in January of 2010. The reporter, Dean Torres, discusses the project in San Diego and it's really worthwhile watching, and has Dr. Stephen Andre from the VA Executive Sponsor of VLER, and Dr. John Maddox, the Assistant Director of Kaiser Permanente, discussing the advantages of the VLER project primarily from the clinician point of view. But regardless, the project is currently active, we're currently sharing

patients, and within the VA we're implementing systems that do give patients the option to allow and present sharing some of their information.

This is an overview slide that just describes the basic features of it, and I'll use it in a little bit to outline the discussion that we're going to have further. At the top you see the NHIN gateway, which is the outward facing component and it includes the policy enforcement point that makes decisions about whether or not that have been made, it enforces the decisions.

The adapter does what it says, it adapts the backend systems so that they can be queried, and the adapter assembles the result into an outgoing message. In this case, the messages are HITSP C32. On the boxes that surround the adapter and the gateway is called the policy enforcement point. The other box, the CPP, which is the consumer preferences and policy area, has a number of components; many of these are management components.

In the bottom area of that box you see E-consent, and the E-consent is speaking to the consumers, the patients, the veterans consent directives that they're electronically creating; that then is sent to the Release of Information Office where it's vetted. So we say that patients submit a request and once it's vetted and the organization has agreed to that request, then it becomes part of the rule set that we would be enforcing.

The ROI Office sends that rule to security management system where it can be implemented in the technical mechanisms of the enforcement component that are illustrated at the top, the PDP and the ADI. And those are just components of the system, the policy decision point that enforces or makes a decision about the rules as to whether or not they're enforceable or not, and tells the PDP the results. You can see much of this is involved with the management of consent directives and the actual enforcement of them is at the top of the chain.

This particular drawing is a conceptual one and I don't intend to imply that this is the design that we have, there may be significant changes to this, but this is the general idea. The result is that what we send currently is the C32 and on the screen now you see a representation of that as a VA clinician might see. Currently the C32 is restricted to certain specific displays here, the allergies, medications, and problems.

That's the introduction; we'll now talk about the foundations. In terms of foundations, our story is built a backbone of the work that ONC has been doing, and particularly within HITSP. In this slide you see a general overview, a bottom of innovation that Dr. Fridsma provided to this committee several weeks ago. I thought it very well illustrated the work that has been going on and I would use this to highlight our activities. Certainly, the VA has adopted or is in the process of adopting the justices NIEM concept and the standards from the Department of Health and Human Services with the NIEM being the National Information Exchange Model.

Saying that HITSP was largely engaged in this, evaluating use cases from HHS and incorporating those in developing standards and producing a number of implementation specifications and constructs that have led to reference implementations and pilots. And are leading now to certification of systems within some of our capabilities to implement a portion of certifications within some of the standards development organizations.

This slide is a very top level view of what I call the system security requirements from the previous model of requirements and use cases is an important starting place to evaluate what you're going to do. And this slide is a very high-level view of that that says that while we need a security and privacy infrastructure for end-to-end data sharing, and that includes the infrastructure of the NHIN, as well as the infrastructure internally throughout your organizations. It also includes the need for high assurance person identifiers across federated domains, organizational and personal policy enforcement accountability through audits, and a number of assurances and interoperability through standards, common processes, and system certification.

The patient privacy requirement care, the key idea that we had been encouraging is the notion that we would enforce both consumer enterprise policy with common security services. And a few years ago, maybe that wasn't so obvious, but once a patient's privacy policy has been vetted by an organization, we would say that it becomes part of the business policy of that organization. And according to HIPAA, we're obligated to enforce it. So the enforcement of that in the system would logically for us, meaning the enforcement in the existing security systems rather than creating a new parallel system.

In this regard, the policy or the rules or the preferences to the patient both control access and constraints existing security policies. By that I mean that a disclosure by the patient is something that an organization wouldn't do on its own without the patient's authorization. And also in general, the patient's ability to make restrictions against to whom or what information might be controlled is largely represented as constraints on existing policies. So we wouldn't say that a patient could give another clinician within an organization the right to write prescriptions, but the patient may say or an oncologist the right to do things, so it's their right that the organization holds. But the patient may say I don't want my oncologist to see some particular information, so they're constraining the rights that the organization has provided.

I've been talking about the use cases and requirements in a very high level, entering Dr. Fridsma's model, and now I'm talking about how standards are related to that. And this is a very important aspect; I'd like to spend a few minutes on this slide. There are a number of standards that have been working for a number of years to develop the capabilities within the healthcare area, and they're illustrated here. What may not be apparent is these standards in the organizations work very closely together. They build complementary and interoperable standards.

For example, the ... anti-insights, the anti-balloon down at the bottom there has really a standard for role-based access control, 359-204. That is the core standard for how to express role-based access control. That particular standard is reflected in health level 7 and health standards developed in an organization, which has produced a healthcare functional role standard that looks to the anti-standard for compliance. This standard is currently in its second revision.

The anti-standard has also been adopted inside of OASIS and within their standards as a profile. So that by adhering to one standard, there's a lot of interoperability achieved and interaction between other standards. So HL-7 has also recently developed a CDA revision to consent directives that you heard about I believe on one of your last calls. We are also developing in HL-7 security and privacy service functional models supporting service oriented architectures. And a number of security and privacy models we're currently finalizing the balancing of a harmonized security and privacy information model. These are very key to interoperability and to sharing data because really the healthcare specific part of the security system is the information model.

Privacy and confidentiality codes have also been developed within HL-7. I'll speak briefly to OASIS. Standards for interoperability, the NHIN is using SAML, XACML, and not yet, but WS-Trust. Within OASIS, we've created a healthcare profile, largely driven by efforts from the health information technology standards panel. I know some of the members here participated in that panel. I participated as one of the principle office for CP20, the access control standard. And we recognized a gap there that we went to OASIS to fill, established a technical committee specifically charged to meet HITSP requirements, validated healthcare profiles of the security assertion markup language, the extensible access control markup language, and provided those to HITSP where they were entered and approved as standards within there.

The WS-Trust is also included in CP20, the access control construct, and it's currently in public review. In ASTM, you see a privileged management in structural roles. There's a standard there for privileged management 2595, which was harmonized with the ISO privileged management in access control standards, the PMAX standards. And you see ISO has also produced structural and functional roles. ASTM has a structural role, a standard 1986, that we'll be talking about later.

So the HITSP work, whether the standards organization has produced dynamically standards to support HITSP, ONC, and NHIN, and has demonstrated the capability to implement those standards. So it's very

important to create standards, but it's also important that they be implemented. So OASIS is largely driven as the vendor consortium, and the requirements to develop a standard there means that you must have its members demonstrate that they can actually implement the standards before it can be validated.

### **David Staggs – SAIC – Consultant**

I'll give Mike a break here. This slide, leveraging standards organizations, we've been working, Mike has been working since 2004 developing standards that are now planned for use in the NHIN pilot. You'll see this slide shows recent activities over the last three years involving the standards organizations, such as the ones Mike described, HL-7, OASIS, and ASTM. And if you look at this timeline, you'll see several interoperability's, the RSA interoperability, London interoperability, another RSA interoperability, and there's the NHIN interoperability in there.

Those focused volunteer efforts to form, test, and validate standards created to fill the gap identified by HITSP. Again, this aligns well with the model presented previously to the committee by Dr. Fridsma. These standards organizations have been very responsive to meeting the challenge in this area and the pace has obviously increased. And as a result we have a reference model available, and we can demonstrate and validate the standards that make the exchange of patient information interoperable between large healthcare organizations.

This is a representation of how the standards work in a clinical setting. We have that list of interoperability's on the left. You'll notice that each one built upon the next starting with the XACML policies, moving to the SAML cross enterprise exchanges, and more recently adding WS-Trust to interpret tokens from different organizations.

Now along the bottom, near the bottom, you'll see the use cases that we started with that are supported. The interoperability's address organizational security and not just in the exchange between organizations, it's within the organization as well. We demonstrated roles and interoperable permissions and how purpose of use changes the applied permission sets, for example, emergency access might have a different result based on a different permission set being substituted. How the approved consent directives are integrated and how applications can make use of this policy-based access control.

How future proof are these standards you might want to know? And at the 2010 XSPA demonstration that focused on WS-Trust, we showed how patient consent records might be used to limit the release of information based on a patient's GNOME. This is an example of what's called a clinical adapted service there in the middle of the diagram that can interpret the patient's intent as new scientific discoveries make more information available from your GNOME. So slowly and steadily we learn more about the risks inherent in our gnomonic makeup, but the patient's intent not to release certain gnomonic information on a susceptibility to a disease is constant. Here we leverage the gnomonic wide association services, the GWAS, to redact the information the patient did not want released.

For example, if susceptibility to schizophrenia. So as the new studies show certain traits of the GNOME can make you more susceptible to schizophrenia, but that new information is also redacted to meet the original intent of the patient preference. This is great, this shows that the standards that we're developing are actually extensible and are not locking us into a certain approach.

Here's a map that shows the location of the participants in these activities. The map shows the distribution of contributors to the interoperability's and the development of the XSPA standards. The four clusters you see in there represent the interoperability's, and this is a great map. During the interoperability's, the services were actually used from around the world over the Internet, there on the floor of whatever conference we might have been at. For example, at the three-day RSA 2010 demonstration of the model, we had remote servers, including the DoD Lab in Arizona providing the EHR, the electronic health record, and the service provider. We used IBM's Australia's site, providing the requestors policy decision point from another organization requesting information on EHR. And we also made use of Jericho Systems Corporation servers in Dallas, Texas to provide the policy decision point on the information holder side.

This is great; this shows the possibility of securely using the Internet and its distributed systems in a way that's going to be scalable and extensible. This also reflects our intent to have a harmonized worldwide approach to privacy and security in the exchange of patient information. In fact, the OASIS standards are now going to ITU for harmonization and adoption in Europe. And as Mike said, we did a lot of work with HL-7 to make sure that these proposals are in line with a worldwide view. Once again, all these demonstrations were conducted through OASIS in support of HITSP.

### **Mike Davis – Veterans Health Administration – Security Architect**

I'll talk to a bit about the implementation efforts that we have ongoing. And to talk to that, I'll go back to that first technical model that we have and describe what we view as the four layers that the systems must implement in order to enforce a patient's consent directives.

I'll start at the bottom layer of this figure and we'll talk to them in more detail in the ensuing slides. The first layer is if the patient, the consumer themselves, who have preferences about how they would like to have their information handled and to whom and what types of preferences that they might have with respect to them. To make this practical in large scale terms, this needs to be able to be created electronically; recognizing that always there's going to be a paper component. But to the extent that we can make the consent directive electronic, we're going to have more efficient workflows, more efficient systems able to process them with less human intervention.

What we're showing here is the ability of a patient in this layer to express their preferences through an E-consent, an electronic consent directive. That would be forwarded then to a privacy management component. A privacy management component is responsible for vetting that particular request within the organization. Within the VA we use the Release of Information Office for this. The Release of Information Office may consult with clinicians, with patient safety, with patient privacy, or other groups, and consult with the patients themselves to determine and make the patient aware of what the implications are of their particular preferences. Some preferences may make perhaps the pass through automatically as approved by the Privacy Management Office, let's say for example, the preference to opt in to participate in the NHIN. Others more in the line of restriction requests might require more intensive review.

Once the Privacy Management Office has made a decision and the organization will accept the policy, then it's passed through the security management component. Security management is the traditional notions of security management within a security system to implement and provision security attributes and rules for the security system. So they would accept the privacy rules that the ROI Office has presented and encode those into the information stores and the policy stores of the access control service, which is the engine that actually operates on the policies.

So at the top level, I'm showing the access control service itself, you would think of that simply as the IT system that receives requests from an external source for information. And then is responsible for making the decision and enforcing that decision and releasing information in response to the request. A simple way in my mind of thinking about this is that this automation system acts like a speaking tool, where the person comes to the door and knocks on the door, and said Joe sent me. The guard who is the policy enforcement point here, turns around to the manager and said, shall I let this guy in? And depending on what the manager says is the rules, he says yes or no, and the guard at the door that the policy enforcement is going to let them in. It's very analogous to what's happening here. You can see that there's a large, you've got three components of security management, privacy management, and consumer preference management that need to be considered to make this work.

I'll talk about the consumer privacy and electronic consent portion. We'll start with presenting this in terms of really what the business is for the VA. On this slide you see the President, who has been approving or assigning of ... this year, giving veterans increased privileges and capabilities doing things to ensure that a new program is in place to provide comprehensive assistance to veterans.

She's shaking his hand, the hand of Sarah Wade, who you may have heard of. But I want to speak to her case a little bit as illustrated, the kind of problem that we're looking at and dealing with, the personal

issues around personal protections of healthcare incarnation. Ted Wade is Sarah Wade's husband, a sergeant serving in the 82<sup>nd</sup> Airborne Division in Iraq, when his Humvee was struck by an IED, an improvised explosive device. He lost much of his right arm and suffered multiple injuries in that attack and including a severe traumatic brain injury. So I'd like to just let Sarah speak to this slide in her own words.

### **Sarah Wade Video**

The last thing that I want to mention has already come up, but I guess I'll just drive it home one more time, is the importance of confidentiality. My husband and I, the first time we discussed this next project that was really I think his only concern, was while Ted thought it was very important that just civilian providers would have access to the military and VA medical record systems. I think there's also times where they really don't need to have access to everything.

And one of the particular situations Ted and I discussed was some of his inpatient medical health records from when he was having complications back in 2005, that if my husband needs to go to the dermatologist, it might be important for them to have a diagnosis or know what medications he's on just for the sake of that they're providing something insensitive to that, and know that there are however complications that could be caused by certain medications. But by no means do they really need to be able to read his inpatient mental health records for your support.

I'm hoping that you all will keep that in mind as the project is moving forward. I know that probably one of the major focuses of all the IT people involved and know that we're entrusting you with quite a bit of information. The last thing that I've—

### **Mike Davis – Veterans Health Administration – Security Architect**

The slide has the length to the video itself and also links to the testimony that Sarah gave to the House.

Within the VA we have established the consumer preferences and the policy project. It's a sub-project of our NHIN VLER efforts with the goal of providing veterans a simple way to create electronically signed and communicate their personal privacy preferences. But also with the intent of meeting ONC consumer preference requirements and recognizing that while veterans are VA's consumers, the goals that we're talking about will probably be going to all NHIN providers. David?

### **David Staggs – SAIC – Consultant**

That's right, so we're now solving Sarah Wade's problems with our E-consent layer of the model, and that's the outwardly taking side the veteran patient will interact with. We provide an electronic workflow, giving the patient the power to dynamically decide who has access of their medical records.

Moving onto these consumer preferences requirements, this is a slide that refers to a paper. ONC released a paper on requirements providing consumer preferences, and this slide shows how the standards we're discussing meet those requirements. You'll see the green circles indicate that we meet the requirements, and the yellow that we partially meet them, the red circle is an area that we don't really address. All of these, the green circles represent the standards that we're discussing that have been harmonized with other standards and then developed into OASIS standards. These are actually demonstrated at interoperability's and can be performed with existing commercial products.

We'll move on, here's an easy slide. This is the patient's view. The point shown here is that to be successful from the patient's perspective, we have to express some privacy policies, should be easy to do, and readily accessible, perhaps by the home computer, and gone is the need for mailing in complex paperwork. The pilot plans to make use of a series of questions presented to the veteran patient to create the consent directive, which is then submitted over the Internet, and then formally reviewed by the Release of Information Office as Mike said. That's the goal.

Of course, there's always a need for paperwork. Currently, the patients have to fill out paper forms to express to opt in and express restrictions to access of their medical health record. As Mike said, we always intend to accept paper requests, but our goal is to streamline the request process and simplify it,

make it accessible through an electronic workflow. The only way we can support an electronic workflow, can the veteran patients privacy preferences be scalable to our 6.5 million patient population. I won't get into the legal aspects of this, but these forms are strictly construed and it takes awhile for them to be developed. So that's one thing to remember going forward. Mike?

#### **Mike Davis – Veterans Health Administration – Security Architect**

This is a representation of how such a system might work to provide an electronic consent directive. The first thing that's involved is that we have to know who the patient is. There needs to be an identity verification process at some level to determine that we know who the patient is, who is actually making an electronic request. In this representation here that the patient has done that posting and now is identifying himself through an authentication service.

What's happening here is that the patient authenticated to some service is able to see the different types of requests that they made or desire to make, selects one of them. The electronic forms repository holds the workflow that would create a form or an electronic representation of the patients consent directive. And the patient would be guided through a series of questions, along with helpful information on what is required to submit their request. We think it would be helpful to have the form pre-populated as much as possible by a demographic service if that's available, and the patient then would complete the workflow, helped as much as possible by the system itself.

At some point, the patient will have completed this, maybe in one or two sessions, or one session, whatever, maybe by altering a form that has already been submitted previously. But in any case, besides that it's complete to their satisfaction and they want to submit it, this implies that they need to apply an electronic signature. The electronic signature is a representation of the patients point signature or a hand signature on a piece of paper. So this is a legal document or a legal decision that it has to be representative of that and it needs to be vetted with the legal office.

Right now this is an area that we're investigating and it's something that the legal office in any organization would have to approve. The system behind that could be any number of things depending upon the level of assurance required for the signature. It could be an "X" in a box like in an end user license agreement; it could be an "X" with a signature from another authority on top of that to bind it like a notary; or it could be a signature based on a signature owned by the veteran themselves.

We're not planning to issue smart cards or anything like that to a large population of veterans, and instead what we're examining is a digital signature that would be VA managed as part of a software PTI. So the veteran's password and ID or their authorization would actually activate that transparently to the veteran and apply a digital signature to the document, which would then be stored in the service. And then the workflow would pass on to deliver that to the Release of Information Office.

There would be a couple of outputs from the process, one would be a humanly readable form that the patient could print out on their own and say, this is what I signed, this is what it looks like. The other might be a representation that would be electronically and semantically interoperable passed to the ROI Office as a CDA release to the CDA consent directives or which could be in fact exchanged between organizations. The idea here though is that the consent itself is important enough that we'd want to bind that consent very closely to the patient and also to the information that's being protected.

I mentioned that the CDA R2, this is the slide that you saw earlier in our presentation regarding the HL-7 efforts. And I've just indicated here that again that standards are key to the interoperability and that we're planning to implement the CDA R2 consent directives as a means of implementing the patients consent directive. While going to the area of privacy management in more detail.

#### **David Staggs – SAIC – Consultant**

Yes, privacy management, this is kind of the back office side of what happens when the E-consent request comes in. Here's the description of that process, consumer preferences and training the ROI consent reconciliation. This is just a diagram of the back office view providing the capabilities to the patient. The consumer preferences are received electronically, patients submit privacy preferences, but

they're not enforced until the organization accepts them. This is similar to what happens with paper requests now, but it's scalable. There's feedback from the privacy professional to the consumer if there is an issue, then the privacy preference is forwarded on to security policy as one that's been vetted and approved for actual use in making the access control decision. That's what we show here.

Let me give another screen shot of one of the back office applications. Here, this is the VA NHIN adapter opt in/opt out application. This is an application used by the VA side for the back office to transfer the patient's privacy request into an approved data store. This process changes these attributes associated with the patient to opt in or opt out to be able to try the exchanging of their medical health records between clinicians they may see in different healthcare organizations.

For example, Kaiser Permanente and the VA in the San Diego pilot. The approved request to opt in or opt out is made by the back office and is then reflected when you happen to be in a different organization and you want your medical information shared with clinicians seeing you; and shared from an organization you've been seen in to the organization you're actually being examined at. These are the elements that we have to also include in this overall system.

Mike, we're running a little bit behind, but here's your slide on the system.

**Mike Davis – Veterans Health Administration – Security Architect**

Okay, we're going to skip over this. This slide simply wraps up what we've been talking about, the role of the consumer and the role of the ROI Office in that. What this slide does show that there is a feedback to the patient once the consent directive has been approved to let them know that it has been accepted. And this is similar to what you might expect as a security check, if you change your password that you're notified that your password has changed. So if there was something wrong, you could get involved.

We'll go into the security management area. The first slide describes security management in general, this is nothing new. But here just for a completeness so that we have a slide that describes what security management involves. I'm going to skip that and go ahead to this slide, which looks very confusing, but the intent is not. This shows structural roles from a security standard. User roles as part of security management need to be assigned, that takes a lot of work, it takes a lot of people. It takes management at a lot of different levels to do.

These roles need to be interoperable and they need to be standards based. ASTM 1986 has for a number of years produced a table within it called persons for whom role-based access control is warranted. These have been mapped previously within the CC codes. During the HITSP development period we found that this standard had not enumerated the roles and so they could not within the context of the OASIS work to create the healthcare profiles, could not be readily specified. And what happened then was that the NHIN specification factory, we looked for codes that could be specified and selected to SNOMED CT, which is not a healthcare security standard.

Within HITSP and OASIS, with respect to the profiles, what we decided to do was to approach ASTM, enumerate the roles and assign an ASTM ... to them so that they could be referenced. We worked with folks on the NHIN spec factory to create the SNOMED links to the codes that were being used to the ASTM codes for backward compatibility purposes. So the OASIS standards specifies the ASTM 1986 as the standard in using that ... within the enumeration within ASTM, but it's fully mapped to the SNOMED CT roles. This was done in a period of about three months, which we could not possibly have modified SNOMED CT during such a short period. But I think the point here is that the standards organizations are constantly evolving and they are in fact working to meet the nation's needs as they are known. And as David said, the pace of this development has increased remarkably.

The linkage of the patient to the information being controlled is very important here, because in the process that we're describing and what we're seeing is that external organizations actually ask for veteran's information based upon the VA's internal identifiers. There's a lengthy process that does that using demographic information between both organizations, so that the patient themselves when they express a patient with a consent, they have to be known. We need to know who they are. Some kind of

identity proofing process is necessary, that process itself will vary depending upon the nature of the information being protected, but the VA or the federal agency applies the NIST 800-53 level to determine assurance levels.

The process of identity proofing applies both to patients and to employees and contractor affiliates and other beneficiaries. It's a similar process for all of them, but it may vary depending on the type of information. So for VA's employees, we're proofing to NIST level 4 issuing personal identity verification and cards from HSPD-12 direction and smart cards to a very high level. For patients who are not doing that, we're issuing a veteran identity card, but it's not widely used. It's not used for electronic purposes, it's used for a patient identification purposes. But regardless, the process here that I'm showing is a process that is currently under development. It's not completed yet within the VA, but it would allow for identity proofing of our veterans.

And the linking of them in a very authoritative way using probabilistic matching techniques to their identity in the electronic health records and to their identity as known by the master patient index. If an external provider is asking the VA for information that they access through that identity known to the master patient index, it has to be closely linked with a commensurate level of assurance to the policy that the patient has presented; otherwise, we have the potential for a mismatch execution of the wrong policy and potentially undesirable consequences.

We've covered the ROI Office of Privacy Management, the access from the patient's point of view, and expressing a consent directive, and now we want to talk to the enforcement and the engines themselves. I'll start with a general overview that this particular diagram is a simple representation that appears in both CP20, the access control construct from HITSP, and then the OASIS standards.

The representation on the left is that the service user or a requestor, a doctor or a clinician, makes a request of a service provider, the person that has the information. And they do this by making a request for specific information, providing information about their identity, who they are, and then they provide additional information about what rights they have to request that information. So these are the authorization attributes.

The service provider is going to take these attributes and go to the access control services in a service oriented way, and ask for a decision regarding whether those attributes are sufficient or to get access to the information that's being requested. It's a process of comparing the users asserted right against what rights are required in order to access that information. And those rights include the management of the rules, the policy, now meaning the rules in the system that had been placed there both for security and privacy. These include the organizational, jurisdictional security and privacy rules, as well as the patients privacy rules that have now been incorporated into the organizations overall security policy. It's all rules suit. The engine doesn't know where they came from, it's simply enforcing them. It makes a decision and enforces that decision so that the request can be fulfilled. David?

#### **David Staggs – SAIC – Consultant**

We can get a little bit more technical here. This slide shows the attributes used in a request between two different providers, two domains. The XSPA standards provide the ability to express this authorization in a number of ways by role, by purpose of use. We talked about emergency access before by organization and location. The XSPA standards provide for close graining access, but they can be extended to find grain control with the use of HL-7 interoperable permissions.

The XSPA standards were created by the OASIS committees to meet the gap specified by HITSP. SAML provides the secure exchange of the request between the organizations, the request for patient data. And the XACML standards specifies the attributed vocabulary, so that we have semantic interoperability. And you can see the standards along the bottom that were involved in developing this model.

The policy comply with the OASIS XSPA profile of XACML for healthcare passed last year. XACML is already in use in other areas. This is a list of policies developed in response to the American Health Information community, healthcare use cases that was created for ONC. All of these use cases have

been demonstrated using the standards on the vendor's products. As Mike said, that's a requirement for an OASIS standard is to have a certain level of vendors that are able to provide the standard.

The policies were done with XACML. There's a standard for that for healthcare, and XACML is already in clinical use operationally in healthcare. One example is the Swedish National Health Service, their XACML is used to enforce policy-based online access to health records exchanged between different care providers in compliance with this strict government regulation similar to HIPAA. So other countries are already using XACML for this purpose and now we can too. The process gives us an interoperable way of doing that.

The XSPA standards are being incorporated into the NHIN connect software used by federal agencies. We have demonstrated a reference implementation in several interoperability's, which is freely available. We have the policies needed for identified healthcare use cases already written and available at no cost for use by the NHIN community and for use by anyone. Only the attributes are loaded and that's what determines the policy decision. The actual policies can be reused. The OASIS is considering making this reference implementation we're discussing, making that in point available online so that vendors can validate their implementation.

Let's talk a little bit more about those demonstrations. Here's a screen shot, we don't have time to show you a live demonstration, so we have some screen shots of one. If you want to see a live one, there is a consumer choice technology hearing coming up that will actually include a demonstration of this technology that you're seeing right here. In this screen shot, you see this screen lets us request information as a clinician would on a patient. This is a case of a cross enterprise lookup as in the NHIN. This means that the request is packaged in a SAML assertion using the XSPA standards, an exchange between the two organizations. And the standards allow the receiving organization to make sense of this request, that's more difficult than it seems. But to understand the attributes associated with the role and the linkage of who's making the request, is the focus of these standards we've been working on.

The result is shown at the bottom. The bottom part is the patient record, the C32, coming across the NHIN. I believe this was taken from the RSA 2010, so we were making use of the DoD adapter for creating the C32, which actually has been redacted; parts of it has been taken out to be consistent with the patient privacy preferences that were set up in the next slide I'll show you. This reference model provides an advance security and privacy in a scalable way that has already been implemented and provides the functionality required to meet the use cases expressed for healthcare.

Here's the provider side. We saw the request from the clinician. We've included in the screen shot showing the provider side hosting the information. This here a security management professional would add the organizational and approved privacy policies. This is a reference implementation, which is available. We created this to have the framework to test the standards. It's not a commercial product. It's freely available to test the standards and to be able to allow other folks to create their own.

The tabs along the top allow us to opt in a patient, add their privacy policies, and it allows restriction of requests to a fine granularity, or it allows restriction by name, role, information requested. This is mostly used to validate the standard and it's been used at several interoperability demonstrations.

Here is a screen shot from the side requesting the information again. Here is an example of a deny returned based on the requestors ASTM role. Depending on the situation, the requestor might have the ability to request the same information again using the emergency purpose of use, there on the right. If they have that role that allows them to assert an emergency, a different set of permissions are applied. Perhaps the patient has said they don't want certain information released, but if it's really an emergency, use these other set of decisions. So that's incorporated in the model as well.

Let's take a little look at the actual policy written in XACML on the right. Here is an example of policy code. In this case if the patient wanted to prevent access to their healthcare record based on a particular role, for example, this will force a deny on a request based on that role. The result is based on the attributes associated with the patients and loaded into the data stores so the policy only needs to be

written once. The policy language is in XACML and this has been profiled in an OASIS standard. So the policies needed in the NHIN pilot have been made available at no cost. The attributes needed to make the access control decision are added during run time and run through the standard templates to make the decision. This could be increased by hardware accelerators.

If you want to see the actual demo, we have excerpts from a live demo available on YouTube, and you can find them by searching for the words OASIS and XSPA. You can also subscribe to the XSPA user to see the entire play list and stay current with new videos. Each video is three to five minutes long and covers in aspect to the XSPA profile and the related use cases. You can see how access requests are made, evaluated and granted or denied based on the selection of privacy policy and organizational policies. It will show a patient making a particular decision and perhaps after consulting with their clinician, going back and changing their decision, opening up their privacy a bit; and the results would be that the second request would succeed so you can walk through the entire step of changing permissions. That's as far as we took it so that we can show that the harmonized standards are complete and provide the minimum subset of what's necessary for supporting the use cases.

### **Mike Davis – Veterans Health Administration – Security Architect**

Within the standards development organization, work continues. As David mentioned, OASIS is looking to formalize the work there into a reference model that can be used for certification purposes. We have ongoing work with hopefully it's in HL-7 enforces development of technology of healthcare ontology's for security based upon fundamentally the HL-7 information models that have been validated there.

The ontology provides very useful benefits to both patients and to the systems enforcing privacy rules. It makes it simpler, ontology's make it simpler in effect for patients to express their preferences. This is transparent to the patient as part of the underlying system to accept the patients consents expressed in their language and then convert that into the technical language that the security system needs in order to enforce it.

The ontology's also provide ways to improve the processing of the mechanical systems themselves to make those decisions quicker and faster without having to look through every possible combination of rules. Within anti-insights we have efforts currently ongoing for what they call next generation role-based access controls. Standards for ISO, and within ISO, defining purpose of use, which the U.S. has had input into. And the standardization and generalization of the XSPA work being up, a specific body of work intended to support HITSP and the NHIN to a more generalized expression that could be applied worldwide.

The lessons learned from our work to date in implementing this body of work is that we believe that there's a need for a strong level of assurance between the consumers identity as a person making a consent like this, and his identity within the health record. I also want to say that the ONC direction so far has not seemed to focus on the use of an electronic signature and consent directives. We think it would be helpful to have additional guidance there or to include the notion of electronic signature as a means of dealing with consent directives in a scalable and friendly way.

Also there's a lot of effort that's needed in the back office effort. When we started to implement the standards that have been developed in the work of HITSP and etc., within the VA it became very apparent that we were having a huge impact on resources and the system. We were asking the ROI Office to increase their workload beyond what they currently have. We were asking the security administrators to assign roles in a very systematic way to VA clinicians in a way that have not been done before and certainly in a different way. And so that has a huge impact that had to be considered and also in terms of writing and provisioning policies.

In summary, we've walked through the four layers of electronic patient consents, starting with the patient's view presenting a flexible system for the patients expressed preferences. These are in HIPAA terms expressed either as authorizations or a restriction request, submitting them to a ROI Office or an office within the organization that adjudicates that request and vets it and discusses and works with the patient to make them sure that they're fully informed of the implications of their request. And then accepting the

request to substantiate these policies or rules into the mechanisms of a system that is capable of enforcing them electronically in real time.

This means the provisioning a security and privacy policy rules themselves and attributes, contextual rules about the organization, the time of day, etc. Rules about the kinds of information and what actions are being requested on that information, the associated attributes, the details. It's Dr. Bob, it's the patient Billy, whatever, that needs to be substantiated, and then the enforcement of a request from a requester to a provider organization.

I realized that we've left many questions unanswered here, and fundamentally the patients desire to control information, and the tension exists between that, and the clinician's desire to access information. We're specifically deferring those important discussions to these committees and to CVHS, HHS, Congress, and others to establish the appropriate balances. However, what we've been describing is a system here that's capable of enforcing those policy decisions when they're made.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, thank you very much. This was an excellent presentation. It really brought together a lot of what we've been talking about and wondering about and have acknowledged as difficult questions around consumer choice and consumer permissions. So let me open it up to the two workgroups and for any questions or request to clarifications, comments.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Wes Rishel.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, Wes.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

This has really been eye opening. I am going to ask some questions, not necessarily about the raw capabilities and standards, but how they're applied in NHIN as it exists today, and issues about rolling it out more broadly. One of the things that I'm not clear on, do the consent rules accompany the data as it goes out and is it incumbent on anyone who receives the data to enforce the consent rule if you're going to pass it on?

So a specific scenario is, I as a patient had a user friendly way of going through a complex hierarchy of roles and have picked out some that can accept and some that can't. A request comes in for my information and the consent engine says, yes, that's okay, we know the role of the requester and that's within the region. The requester gets it, it becomes a part of the record of the requester. And then later on there's a request for information that goes to the middle party there. Do they have to enforce the original consent rules that were applied by the patient in the original source organization?

**Mike Davis – Veterans Health Administration – Security Architect**

Thanks, Wes. I think I understand what you're asking. In a sense what you're asking is a question about policies.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I understand that the dancer is frequently, here's a technology, you figure out the policy, you use it, but I am more or less asking how you are using it with Kaiser now? That is, what are the policies you've put in place? And then I guess the secondary question is what is the breadth of policy that the technology would handle?

**Mike Davis – Veterans Health Administration – Security Architect**

Okay, so when you ask about what we're doing now, we're essentially complying with the laws that exist, the specifications of the NHIN, and the data use and reciprocal support agreement. So within the context of that consignment, the VA is doing authorizations primarily because of a requirement of law having to do with the United States Code Title 38, Article 7332. And because of that, we're asking for patient

authorizations to opt in to the exchange of their information over the NHIN. So currently all patients execute an authorization for a patient policy of opt in. That's currently the policy that is operational and the pilot in San Diego that is applied both by Kaiser and by the VA.

According to the DURSA rules and according to the specifications of the NHIN right now, we do not share the patient privacy across organizations. It is technically feasible to do that and clearly HITSP has provided ways in TP30 to share that information and the CDA R2 consent directive provides ways of encoding that in an interoperable way, but that's currently not done. The DURSA rules in fact specify that each organization is free to accept or deny information based on their own policies, not knowing because NHIN is a nationwide network with a variety of policies enforced by different states, and so these rules maybe different that organizations must comply with.

The answer is that currently we're not passing the patient authorizations across and we don't have any expectations that another organization would enforce the consent directive that was given to the VA. But I would just point back to the ONC of consumer preferences requirements draft document, which is still being worked on, that does indicate that ONC sees the need to pass these policies between organizations and some of the workflows at least in the draft indicated that kind of capability. But if you ask about it today right now what we're enforcing, so I'm answering that very specifically.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay. My other question then was I'm just trying to understand, it's really great to see your show of how it works in the VA, because it shows the complexity of a large organization. I'm trying to imagine this process in a small doctor's office where right now the consent engine is the clerk in the back room. What would it take in your view to scale this down to software that would be sufficiently simplified to work in a small organization?

**Mike Davis – Veterans Health Administration – Security Architect**

The scalability here may occur on several different levels, one would be a large organization level, one would be maybe a medium level, and one would be a very small level. Currently right now there are efforts to deal with the small caregiver and the efforts of NHIN direct provide immediate and easily scalable mechanisms to share information clearly. And organizations of that size, the need for something as elaborated of what I've been talking about may not exist.

In a medium organization, somewhere between a small provider and a large provider, maybe a single hospital or a group of hospitals, something more akin to the NHIN might be appropriate. We've envisioned the notion that we could have something like a provider who has a commercial EHR product. There could be something such as a NHIN set top box, essentially a commercially available product that has the adapter and gateway built into it that you plug in and tune to the EHR. One of the CCHIT certified EHRs that have been identified just like you program your VCR at home or a universal remote control to accept any number of different inputs.

I think that the answer is that we have not got to the point yet where we can categorically say that we can take something that I'm describing and scale it down to a single practitioner office; maybe that's the wrong solution, I don't know.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Is there a requirement to generate additional meta information that goes with the data?

**Mike Davis – Veterans Health Administration – Security Architect**

Currently there is a certain amount of meta information that's provided with the C32 or can be provided. We're at least providing currently in the C32 a source location from where that data came. Other demographic information about the patient can be provided as well, but currently that's what we're producing.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

But no meta information about the role, the sensitivity of the data, anything like that?

**Mike Davis – Veterans Health Administration – Security Architect**

In the response, you're asking?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes, well it can be response or it can be an unsolicited output, but in either way it's with the outgoing data.

**Mike Davis – Veterans Health Administration – Security Architect**

What happens here, Wes, is that the clinician makes a request, he provides his authorization attributes, his right to request that. And the system is simply matching that against what the policy says has to be expressed to get access to that. It's just an equation to the X equal block, and it makes that decision. When the decision is made, the output is the information that the clinician requested and no more. It's simply the report currently that we're producing that is the C32, so that's what is given.

Now there's clearly a potential to do other things, but right now to pass back the patient policy with it, but we're not doing that.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

So the example from Mrs. Wade was the C32 might be a note that describes a session in let's say drug rehab or something like that.

**Mike Davis – Veterans Health Administration – Security Architect**

Right.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

That might have medications, it might have progress notes, it might have several things in it.

**Mike Davis – Veterans Health Administration – Security Architect**

Right.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

But that codification of what makes it sensitive is not required to be sent, is it? The receiver will receive the data and then do their own codification of what makes it sensitive.

**Mike Davis – Veterans Health Administration – Security Architect**

Right. We're not sending the codification of the data currently back with it.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

The codification advise, it's some sort of indication that this is sensitive data.

**Mike Davis – Veterans Health Administration – Security Architect**

Yes, I want to address that point basically. The security system responds and processes rules that it knows, but the security system isn't an EHR, it's a mechanical security system. So it has no way of knowing what the sensitivity of the information is. It relies on the underlying EHR to tell it. So if we're discussing sensitive information of a particular category, let's say particularly in the VA's case protected information on your 7332 HIV, sickle-cell, this kind of thing.

There's no way for the security system to look at data that's been received and say, that's HIV, that's not what the security system does. The security system has to be told by a label or by some rule or some mechanism that this information that I'm giving you is HIV or other sensitive information. Then based on the rules that it has, it can apply the rule to that particular data, but it has no way intrinsically within a security system to look at data and make those kind of decisions. It relies, like I said, fundamentally—

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Basis, so then it's an obligation of any EHR that works with this system to provide that coded information about the sensitivity to the security system.

**Mike Davis – Veterans Health Administration – Security Architect**

That's right. So the security system could be told and we've done this with respect to C32, the patients request is to not pass let's say medication information in the C32. So the security system knows what that is in terms of the C32, and so we could redact that or block that from being transmitted as a group, because it's a defined object. So security has to work against defined-known objects. We have no ability currently to look at data and say, this is this type of text.

We have been, by the way, examining that, and there are mechanisms that might be possible in the future to do that, but we currently do not have that in any kind of operational state.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay, thanks.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

This is David McCallie. Can I ask a question, Dixie?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, please do.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Mike and David, first, thank you for an extremely well-organized and clear presentation of a subject matter that's bewilderingly complex, at least in terms of standards bodies and three and four letter acronyms involved. I think I learned a lot that I didn't know, including knowledge of the XSPA, which was new to me. So that alone is worth the price of admission. But my question is just kind of a judgment question.

One of the side effects of the design or of the approach taken so far by the NHIN is that a patient who is mobile, which certainly a service person could be; but also an ordinary and not a civilian, who moves in a variety of different places, could end up with their data spread out all over the country in three, four, five, or six even. If you live in a border state like Kansas City where you may get care with providers in the Kansas side and the Missouri side. You could end up with your data spread out all over the place. Some of us personally consider that maybe to be a flaw in the design of the NHIN, but whatever, it's the way it is right now. And until the fundamentals change, we have to deal with it.

The question is, when we reach the point of where we would like to share our consent policies across all those domains, notwithstanding the differences in policy at a state level about what the consumer actually has the right to control. Assuming the consumer is making reasonable requests and they wish to share across all those domains, my question longwindedly, sorry, is, how close do you think we are with the standards that you described to making that technically possible? And how close with the ontology's and code sets are we to making it implementable possible? Put policy aside, assuming everything is done according to the policy requirements. Are we technically capable of doing a distributed consent management and do we have the content in the ontology's and code sets necessary that if the states wanted to implement it, they could do so? I apologize for the vagueness of the question, but hopefully it's clear where I'm headed.

**Mike Davis – Veterans Health Administration – Security Architect**

That's a tough question. I'll address the aspects of it. I'm not sure I'm capable of answering the question in its entirety. I've been working with standards for a number of years, produced 11 standards, some of which have been accepted by the NHIN. If I were to start all over again, I would have started with developing the fundamental information model and ontology's that healthcare needed. I wasn't smart enough to do that and we worked a lot in the technology area. And we've come lately to realize that it's all about the information and the information models more than the technology.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes, good point.

**Mike Davis – Veterans Health Administration – Security Architect**

I think that in answer to your question in part that there are standards today that are certainly capable of representing patient policies to a considerable degree of granularity. The probably issue that I was just discussing with Wes about the capability of back end EHRs to actually provide the distinction of between different types of information. And we've been focusing primarily on directly labeled information, this is HIV, this is whatever; and not the secondary level of inferences that might be made, if you have this particular prescription for this particular drug, I can make an inference. And you have to remember that clinicians are inference engines. This is what they do.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes, just to back that up, we run a local thing here in Kansas City with a number of the self-insured employers that's a lightweight health information organization. And one of the people on my team is responsible every quarter for updating the list of drugs that are considered to be sensitive drugs. And it's a phenomenally complex process of inference based on what does this drug mean in terms of assumptions that a clinician might make about diseases that are being treated by that drug. And many drugs obviously serve many purposes. So if four-fifth of the purposes are generally benign and non-sensitive of one-fifth or sensitive, does that drug get restricted or not? And it's an incredibly thorny question, I certainly sympathize with that point.

**Mike Davis – Veterans Health Administration – Security Architect**

Right. So we've been focusing on the first layer, the things that are explicitly known to be sensitive and not the inferences of them as the first step in the process. With respect to the patient's ability to create and manage their privacy preferences across multiple organizations, I think that there are emerging capabilities in commercial PHRs potentially to do that. I won't mention names, but there are a number of them out there.

The fundamental issues has to do with really the policies. Under current HIPAA rules for treatment purposes, no authorization is even required or an opt in required. The VA is doing this because of specific legal constraints that we have. And then the DURSA provides that each organization enforces policies based on their own internal decision. The patient unfortunately in this environment has no expectation that they can create a policy that is uniformly enforced across all the jurisdictional, organizational, and policy lines. So they can make a request, but the results of that request may vary differently by different organizations.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Yes. And that's a fundamental flaw with this distributed model that obviously no amount of technology is going to fix that.

**Mike Davis – Veterans Health Administration – Security Architect**

That's right. So I would say that the issue isn't the technology. Back to the question, if the policies that we as a nation decide to implement give the patients these rights, and we learn how to balance the tension between the patients request and the need to provide healthcare and do no harm, then I think we can have mechanisms to enforce that. And we have recommendations from the NCVHS on how that might be addressed.

We've looked at that as well. It's where rather than redacting information from a request, we may protect it in some manner and send it anyway, but it may be encrypted within the message requiring additional permissions to get to, under a different purpose of use data, emergency access, or it may be hidden behind a great glass barrier, this kind of thing. Those are policy things and I think there are technology answers that are capable to devise to answer those.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

That was going to be my second question, and if I've taken up too much time, you can defer. I was wondering if you have looked into a digitalized management style approach where the permissions actually are carried or the document and it's been tested has to ask a central service before it would let you view it; where the permissions are actually embedded in the document rather than in a policy enforcement point that the EMR has to be taught how to interact with.

**Mike Davis – Veterans Health Administration – Security Architect**

We have looked at those technologies. They were discussed in HITSP. There are certainly active discussions among the various groups. Within the VA we have looked, my organization has specifically examined these types of technologies in the healthcare setting. We certainly believe that there is a potential for the use of the DRM type of technologies. We're not suggesting them at this time because of concerns regarding inadvertently denying information from clinicians and then getting access to that at appropriate times, the complexity of the management of that. And because frankly the current laws that we're dealing with don't really give us the leverage to implement such a system.

Clearly, there's a lot of attractiveness in having the policy go with the data that would address some of the questions that you and Wes have asked regarding the enforcement of that information once it's released and it's in the hands of another organization. At the current time, the simple answer is that in a very complex world, the security mechanisms that I've been discussing in an SOA way provide a relatively simple extension of existing security technology and practices that would fit well within the context of an overall organization security.

My organization in VA does not only do healthcare, we have other business needs in the security system that we plan to employ within all of those needs, not just the healthcare needs. There is certainly in terms of OASIS and the policies that we've described that the mechanisms that we're talking about are readily extensible to provide extensions into the DRM type of capabilities.

**David McCallie – Cerner Corporation – Vice President of Medical Informatics**

Thanks. I appreciate all that data.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

This is Dixie Baker. I have another question that's related to both Wes and David's, and that has to do with the ontology. And I recognize that it's still in development and I also recognize that ontology's tend to always be in development, continually changing, being updated. So I'm wondering do you envision the consent directive document actually containing a link to the version of the ontology that was in effect at the time the permissions were given? Kind of how do you see that happening?

**Mike Davis – Veterans Health Administration – Security Architect**

Yes. Without having completed the work and just starting it, we had two motivations in HL-7 where these projects, two ontology projects in HL-7, one in a service oriented architecture and one within the security and the privacy groups. It's a collaborative effort between them. The privacy group is specifically interested in ontology's of the information model as a way to mitigate and make it easier for patients to express consent directives, so that they can use the terminology that the system will understand, inherent other terms or concepts underneath it without the patient having to explicitly express all of those things. So that's what we're hoping to do in the privacy sense.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

And someone would be the holder of the ontology and evolve its versions similar to HL-7.

**Mike Davis – Veterans Health Administration – Security Architect**

Yes. The project is to create a standard within HL-7 to the healthcare organization. And it would leverage the information models that are already validated there, and extend them into an ontology standard that would be part of HL-7's overall architecture. The services are where enterprise architecture framework.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay.

**Mike Davis – Veterans Health Administration – Security Architect**

This is an artifact that we would produce based on the information model and it would be maintained. We have been discussing the possibility of moving some of these models into something like SNOMED CT in the future or building relationships with SNOMED CT; seeing if it might be possible to do that, recognizing that SNOMED CT models really are not security models. It's not what SNOMED CT is about. But they have indicated a willingness there to potentially look at our ontology's and there may be a path there. But right now, these are approved projects within HL-7 that are going forward. They're long-term projects. We recognize the complexity of them. We don't see that it's something that's going to be available tomorrow, but we do see the importance of them as a way of simplifying the complexities in terms of the patient's viewpoints.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Thank you. Are there other questions from our group.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Dixie, I've got another one, but I don't want to double dip, and I'll pause and let anybody else ask who wants to.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

It sounds like you get the next dip.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay. I actually have, I had two questions and I lost one here. What I have is, I know what the first question was, in the United States there is the national provider identifier which has an ontology of provider roles effectively optimized for how to build for provider services. Is there a reason why you chose the SNOMED roles rather than that, and has anyone looked into a mapping between the two?

**Mike Davis – Veterans Health Administration – Security Architect**

Thanks, that's a great question. It wouldn't have been our preference to use the SNOMED codes for user roles. That was a decision of the NHIN specification factory, lacking in their mind a reasonable alternative. In XSPA and OASIS, when we created the XSPA standards we did work with them, had representatives there, and we pursued the identification of a security standard, the ASTM 1986, for structural roles that would be used and maintained. So ... it's not security. All the different standards not intended for this purpose.

The ASTM standard is, but it didn't have an identifier, an OID. It wasn't enumerated so it wasn't adequate. So our work was to go back to ASTM, I was a member and the members of this committee were members, we went back to ASTM, we enumerated the roles there, we mapped them to SNOMED CT. There is a mapping, we had previously done a mapping to the code that you mentioned as well; although that's not currently specified in the standards. Because those codes tend to be not under the control of a standards organization and can change radically, we felt that it would be better to use a security standard specifically for that purpose, because that's what they were going to be used for; that was mappable to other code sets, but that could be maintained within the security realm.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

I'm not sure we're talking about the same thing. I'm talking about the HIPAA provider and numeration where there's an ontology of provider roles that is very large in terms of the number of roles that they're defined and is required for use in various billing processes.

**Mike Davis – Veterans Health Administration – Security Architect**

Right. I believe they're referring to the national uniform clinics committees roles that are accepted by HIPAA, right?

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Yes.

**Mike Davis – Veterans Health Administration – Security Architect**

Yes, that's what I'm talking about.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Okay, alright. I got lost how ASTM came into that, that's all.

**Mike Davis – Veterans Health Administration – Security Architect**

Okay, sorry. There are available mappings, but the decisions and the discussions among a number of parties who examined this in the ASTM standards development organizations was not to use those codes for security purposes, because they're used for other purposes. But to show that there was a mapping, but to use a security standard to specify security roles.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

But SNOMED isn't a security standard either.

**Mike Davis – Veterans Health Administration – Security Architect**

That's correct. And that's why we've taken the action to update ASTM so that it could be used and made it compatible with what the NHIN as a community has specified. Because they didn't have a choice when they needed to make a decision, so they made one. So we hopefully and XSPA specifies this, and I think further versions of like NHIN connect will specify XSPA, and so you'll be able to use this in the future, a more flexible security standard than the limited set that is available from interpreting SNOMED CT in a way that it wasn't intended.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Thanks. Then Dixie, I just have a soapbox statement here for a minute, then I hope the committee will consider. Echoing David McCallie, Mike and the other David here have done a wonderful job at providing a reference that we can use. Sort of like pulling out the roadmap when you're not sure where you are, and describing a process that has come a long way towards providing mechanisms that are robust with respect to variations and policies.

This is important, because we, the federal advisory committees, are sort of right on the cusp of trying to effectively cross create cross understandings between those who think about policy and those who think about implementation of what's feasible. There is some ability for the policymakers to understand the timeframe where a particular approach to policy could be ruled out. Some policy ideas may take longer to be implemented than others. I just want to make sure when we look at it from that point of view we recognize that, and Mike you can give me your disagreement if you disagree.

The point in time that Mike is deciding for this, where the ontology's in process or works in process, some set of vendors that are members of OASIS have demonstrated at running in code, but haven't put it into their standard product releases or educated their field support people on how to install it. And that release hasn't gone through the year to two years it takes for a vendor to rollout its release to its customers in the field. Anything we would decide that relies on this flexibility we should be targeting for implementing roughly four to five years from now.

And Mike, if you think I'm overstating sort of the downstream consequences or the exact state of the development, let me know, but that's my take on the discussion today.

**Mike Davis – Veterans Health Administration – Security Architect**

I would like to address that. I believe that the fundamental standards that we need to implement, a reasonable set of policies that we described, opt in with the exclusions, restriction based on user name, restriction based on user role, organization, location, etc. are here. More problematical issues surrounding the protection of sensitive information and categorization of information and specific

segments, with respect to the products, the vendor's products that we've used have been commercial products. In the demonstrations, these are not cobbled together things.

For example, Jericho has provided to NHIN connect their PDP, their policy decision point, pre-populated with all of the policies that I just enumerated. In fact, the VA is considering the implementation of that or the implementation of commercial products from other vendors that are readily available. If I gave the impression that otherwise, I apologize, but these are plug replaceable and the architecture that we've been describing. There are vendor products today available on the free ones from NHIN connect with the policies that I've been describing.

The ontology efforts, in a longer term efforts, but we don't need to wait for that to complete to start our work. In terms of Dr. Fridsma drawing, we've created the standards, the interface specifications, we've done demonstrations. And now in terms of the pilots that I've been speaking about just in VA and I'm sure there are others, we're actually attempting to implement this using commercial products, in an operational state, in the VA systems, and exchanging data in these policies today.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Mike, I'm sorry, go ahead and finish.

**Mike Davis – Veterans Health Administration – Security Architect**

I'm done.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Great. When I was talking about products, I wasn't talking about modules that sit in the security stack. I was talking about application products that must be modified to work according to these new protocols, primarily EHRs. It has been the experience of many clients of EHR vendors, and even those HIE software vendors, that they go to a tradeshow and they see something running in the demonstration mode on the show floor, and they call up their vendor and they say, "I want that," and the vendor says, "What?" It worked back from the support organization into the development organization. They find out, oh, yes, we did that code based on our standard product and we think we might include that in the release that's scheduled for 18 months from now.

And then there is that lag followed by the lag of rolling that release out. And that is my concern in terms of a rapid rollout.

**Mike Davis – Veterans Health Administration – Security Architect**

Alright. I agree with what you're saying that if the solutions are to be implemented inside of the EHR and requires modifications to those, that's an issue. What I think we've been discussing and the approach that we have here, and my claim that we can implement this without wholesale rewriting of the EHRs is a service layer. Where the policies are maintained at a national level, that the backend EHR is not responsible for enforcing these. These are the responsibility of a service layer, so that if it's an in-tiered type approach where the adapter is asking the backend systems to do nothing more than to provide the information requests and then assembles it into a composite report.

It's the security layer now where the policies, this new security layer, the oriented service layer, where the policies are managed and maintained. So if you take this kind of approach you don't have to modify the EHR. The policies are managed by the service layer, they're instantiated there. And the advantages of that is that you can create the policies, and particularly the patient privacy policies that effect the entire organization in every application or system that may contain patient information that's used to construct a response back to the request.

One way of looking at that, yes, if you're implementing it in an EHR itself, you may require significant efforts. If you're looking at putting a layer like the NHIN in, which has the PDP or the PDP built into it, and all we've done is extract that out into a service layer at the enterprise level, then the policy and the enforcement can be done there. The backend applications and data don't have to necessarily know or instantiate those policies in each of thousands of potentially backend applications.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

Dixie, we're out of time, I think that—

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes, we are out of time.

**Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst**

—it would be great for us to be able to follow up on that, because that's a very interesting line of discussions.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Yes. And I think that it's also a good segue into something I wanted to point out to everybody on this call, and that is as Mike mentioned, there is a hearing on consumer choice technology that's scheduled for Tuesday, June 29<sup>th</sup>. And as Mike mentioned, he's part of that hearing and will be doing a demonstration of the VA's work. And I'm sure that that will be really informative to everybody here, especially having heard the excellent explanation that he and David gave us today.

That hearing on the 29<sup>th</sup>, and it's an all-day hearing, it begins at 8:00 a.m. to 5:15 p.m. Eastern time. It's at the Grand Hyatt Hotel, and to get more information about it, just go to the ONC site. And I think that that's a perfect kind of a forum for us to continue exactly the kind of discussions that you've raised here at the end with, so I appreciate that.

**Mike Davis – Veterans Health Administration – Security Architect**

I was just asking that, but we're doing this discussion with representatives from the DoD, and we're specifically using the DoD's office system as the backend EHR, and enforcing the patient policies without modification to that system.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Great. I'm really looking forward to seeing that, Mike. And again, I thank you and David tremendously. Judy Sparrow is not here to close this, so I want to open this to public comment. So Chris could you do that please?

**Chris Weaver – Altarum**

Certainly, Dixie. If anybody would like to make a public comment at this time, please press star one on your telephone keypad to indicate that you'd like to do so. If you're online and would like to make a comment, you must dial in, and that's 1-877-705-2976, and once you've dialed in, press star one to indicate that you would like to make a comment.

Dixie, while we're waiting for anyone to queue up, do you want to make any wrap up comments?

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Other than what I just said that we're going to have the consumer choice technology hearing, and to once again thank Mike and David for an excellent, very articulate, and informative presentation, we appreciate it. Okay? Alright.

**Chris Weaver - Altarum**

Just giving it another few seconds to see if anyone queued up. It looks like we have no public comments today.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, Chris—

**Moderator**

Chris, one moment, I'm sorry, we do have a public comment.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay.

**Chris Weaver - Altarum**

Here we go.

**Moderator**

From Tom Davidson, Social Security Administration, please proceed with your comment.

**Tom Davidson – Social Security Administration**

Thank you. I just wanted to point out, the question was raised earlier with regards to the provider taxonomy and the NUCC list. And the only thing that I wanted to mention is that that list currently deals well with healthcare providers and their use of medical information, but does not do well with other uses of medical information. And the roles that are involved in that use of information currently, which is probably one of the reasons why the NHIN exchange chose a different ontology set for their roles.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Okay, thank you, Tom. We appreciate that.

**Chris Weaver - Altarum**

Melissa, do we have any other public comments?

**Moderator**

No more comments.

**Chris Weaver - Altarum**

Okay, Dixie.

**Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences**

Thank you. Thank you all for dialing in, and thank you, Chris, for your help as well.